UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/002,697	10/31/2001	Richard Paul Tarquini	10002019-1	4671

7590 03/25/2005

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER	
SON, LINH L D	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 03/25/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/002,697	TARQUINI, RICHARD PAUL	
	Examiner	Art Unit	
	Linh Son	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 October 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This written action is responding to the application filed on 10/31/2001.

2. Claims 1-20 are pending.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-20 are rejected under 35 U.S.C. 102(e) as being anticipated by Vaidya, US Patent No. 6279113.

5. As per claims 1 and 17, Vaidya teaches "A method of identifying data in a network exploit, comprising: receiving a packet by an intrusion prevention system maintained by a node of a network (Col 6 lines 57-59, and Fig 3 #58), the intrusion prevention system bound to a media access control driver and a protocol driver (Col 7 lines 12-24); invoking a signature analysis algorithm by the intrusion prevention system (Col 6 lines 18-21, and Col 7 lines 32-36); and comparing the packet by the intrusion prevention system with a first rule set comprising a rule logically defining a packet

signature (Col 7 lines 32-36).

6. As per claim 2, Vaidya teaches "The method according to claim 1, wherein receiving a packet by an intrusion prevention system further comprises receiving a packet originating from the node" in (Col 5 lines 54-60).

7. As per claim 3, Vaidya teaches "The method according to claim 1, wherein receiving a packet by an intrusion prevention system further comprises receiving a packet originating from a source external to the node, the packet addressed to the node" in (Col 5 lines 54-60).

8. As per claim 4, Vaidya teaches "The method according to claim 1, further comprising discarding the packet upon determination that a signature of the packet corresponds to the rule" in (Col 7 lines 5-10).

9. As per claim 5, Vaidya teaches "The method according to claim 1, wherein comparing the packet by an intrusion prevention system with a first rule set further comprises comparing the packet by the intrusion prevention system with a second rule set upon determination that a signature of the packet does not correspond to a rule of the first rule set" in (Col 7 lines 12-24).

10. As per claim 6, Vaidya teaches "The method according to claim 1, wherein comparing the packet by the intrusion prevention system with a first rule set further comprises comparing the packet by the intrusion prevention system with a rule set comprising a plurality of rules each respectively comprising machine-readable code logically defining a packet signature" in (Col 7 lines 12-24, Col 6 lines 27-35).

11. As per claim 7, Vaidya teaches "A node of a network maintaining an instance of an intrusion prevention system for identifying data in a network exploit, the node comprising: a central processing unit (Fig 2 #39, and Col 6 lines 53-56); a memory module for storing data in machine-readable format for retrieval and execution by the central processing unit (Col 6 lines 53-56); and an operating system comprising a network stack comprising a protocol driver (Fig 2 #30, #34, and #36, and Col 6 lines 11-18), a media access control driver and an instance of the intrusion prevention system bound to the protocol driver and the media access control driver (Col 7 lines 12-24), the intrusion prevention system comprising an associative process engine and an input/output control layer, the input/output control layer operable to receive a signature file generated from a network exploit rule comprising an operand, an operator and a mask (Col 7 lines 24-36, Col 6 lines 7-11, and Col 10 lines 25-45), the input/output control layer operable to pass the signature file to the associative process engine (Col 6 line 53 to Col 7 line10), the associative process engine operable to analyze a data packet with the signature file and assign a logical value to the signature file dependent

upon a result from the analysis (Col 11 lines 15-50).

12. As per claim 8, Vaidya teaches "The node according to claim 7, wherein the exploit rule further comprises a composite of a plurality of rules, each rule comprising an operand, an operator and a mask and having a logical value, each of the plurality of rules being logically connected with at least one of the other plurality of rules by a non-bitwise boolean operator, the logical value of the signature file dependent on the logical value of each of the plurality of rules" in (Col 9 lines 25-45).

13. As per claim 9, Vaidya teaches "The node according to claim 7, wherein the operand comprises network frame data, the operator comprises a bitwise operation, and the mask comprises an operator mask" in (Col 9 lines 25-45).

14. As per claim 10, Vaidya teaches "The node according to claim 7, wherein the network control layer is operable to receive a plurality of signature files each respectively generated from a network exploit rule" in (Col 6 lines 1-10).

15. As per claim 11, Vaidya teaches "The node according to claim 10, wherein a parametric association is assigned to a subset of the plurality of signature files, the associative process engine operable to determine a parametric value of the packet and to analyze the packet with the subset of the signature files when the parametric association of the signature files coincide with the parametric value of the packet" in

(Col 14 line 65 to Col 15 line 5).

16. As per claim 12, Vaidya teaches "The node according to claim 11, wherein the parametric value of the packet is obtained from link-layer header information of the packet" in (Col 10 lines 31).

17. As per claim 13, Vaidya teaches "The node according to claim 11, wherein a plurality of parametric associations are respectively assigned to a plurality of subsets of signature files" in (Col 10 lines 40-45).

18. As per claim 14, Vaidya teaches "The node according to claim 11, wherein the parametric association is one of a plurality of parametric associations, each of the plurality of parametric associations comprising a common subset of signature files, each signature file of the common subset respectively analyzed by the associative process engine against the network packet prior to analyzation of any other signature files of any other subsets of signature files" in (Col 14 line 65 to Col 15 line 5).

19. As per claim 15, Vaidya teaches "The node according to claim 10, further comprising a table maintained in the memory module, the table comprising a plurality of indices each respectively indexing a subset of the plurality of subsets of signature files" in (Col 6 lines 26-43).

20. As per claim 16, Vaidya teaches "The node according to claim 7, wherein the intrusion prevention system further comprises an intrusion event manager, the associative process engine operable to communicate that the analysis of the packet indicates a correspondence with the signature file, the intrusion event manager operable to generate an alert that is transmitted from the node to at least one of a management node in a network and an event database maintained by the node" in (Col 6 lines 20-26, and lines 27-56).

21. As per claim 18, Vaidya teaches "The computer readable medium according to claim 17, further comprising a set of instructions that, when executed by the processor, cause the processor to perform the computer method of determining whether a correspondence between a signature of the data packet and the at least one signature files exists" in (Col 6 lines 1-20).

22. As per claim 19, Vaidya teaches "The computer readable medium according to claim 17, further comprising a set of instructions that, when executed by the processor, cause the processor to perform the computer method of comparing the data packet with each signature file of the selected set of the plurality of signature files" in (Col 6 lines 1-20).

23. As per claim 20, The computer readable medium according to claim 19, further comprising a set of instructions that, when executed by the processor, cause the

processor to perform the computer method of: upon determining that no correspondence exists between the signature of the data packet and the signature files of the selected set of the plurality of signature files, selecting a second set of signature files from the plurality of sets of signature files; and comparing the signature of the data packet to at least one signature file of the second set of signature files" in (Col 6 lines 1-25).

Conclusion

24. Any inquiry concerning this communication from the examiner should be directed to Linh Son whose telephone number is (571)-271-3856.

25. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor Kim Y. Vu can be reached at (571)-272-3859. The fax numbers for this group are (703)-872-9306 (official fax). Any inquiry of general nature or relating to the status of this application or proceeding should be directed to the group receptionist whose telephone number is (571)-272-2100.

26. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval IPAIR.I system. Status information for published applications may be obtained from either Private PMR or Public PMR. Status information for unpublished applications is available through Private PMR only. For more information about the PAIR system, see http://pzr-direct.uspto.gov. Should you

have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

AU 2135

Linh LD Son

Patent Examiner